PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-265866

(43)Date of publication of application : 15.10.1993

(51)Int.Cl. G06F 12/14
G06F 12/16
G06F 15/78

(21)Application number : 04-063964

(22)Date of filing : 19.03.1992

(71)Applicant : CSK CORP

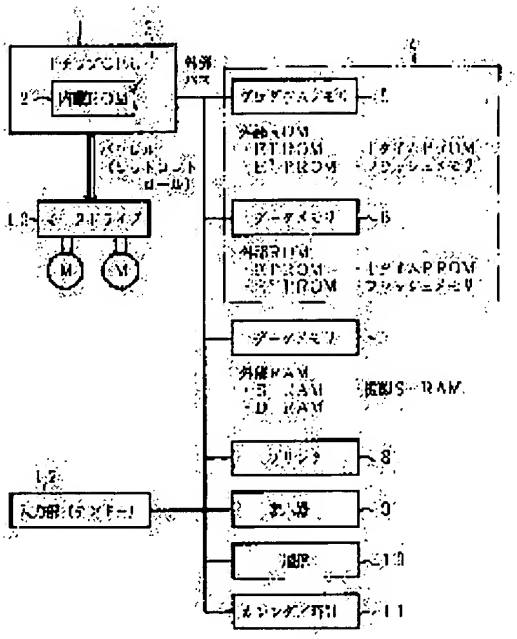
(72)Inventor : KAWAMURA TAKAYUKI

(54) SECURITY SYSTEM FOR EXTERNAL ROM

(57)Abstract:

PURPOSE: To secure the security of data by providing a check means (program) for the fixed data area of an external ROM in a built-in ROM.

CONSTITUTION: A built-in ROM 2 is provided with a check means (program) 2, compares fixed data stored in an external ROM 4 with data in the built-in ROM 2 and checks whether those data are coincident with each other or not. Namely, while the program is executed, the check means 3 checks whether the fixed data in the fixed data area of the external ROM 4 recognized by a one-chip CPU (microcomputer) 1 are fixed data set in advance or not, namely, checks the fixed data at a fixed address, fixed data stored in an auxiliary area, data on the counter number of bytes in the auxiliary area, and error detecting codes to all the areas provided in the external ROM 4. When any one of these elements is not coincident, the one-chip CPU 1 is turned to a held state, and the operation of the entire program is stopped.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of

rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The security system of the exterior ROM characterized by forming the check means of the fixed-data field of said exterior ROM in said built-in ROM while providing the exterior ROM which has the fixed-data field which was connected to the constituted built-in ROM and said 1 chip CPU, and was set up beforehand so that it might be built in the 1 chip CPU and read-out could not be carried out from the outside.
[Claim 2] The security system of the exterior ROM according to claim 1 characterized by storing the fixed data of the fixed address for performing the comparison with the data of the built-in ROM beforehand set as the fixed-data field of said exterior ROM.
[Claim 3] The security system of the exterior ROM according to claim 1 to 2 characterized by storing in the fixed-data field of said exterior ROM the fixed data stored in the reserve field which the exterior ROM concerned has.
[Claim 4] The security system of the exterior ROM according to claim 1 to 3 characterized by storing in the fixed-data field of said exterior ROM the number-of-counts data of the byte count of the reserve field which the exterior ROM concerned has.
[Claim 5] The security system of the exterior ROM according to claim 1 to 4 characterized by storing in the fixed-data field of said exterior ROM the error detection sign to all the fields that the exterior ROM concerned has.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to the security system of the exterior ROM which raised the confidentiality of Exterior ROM, and safety in the ROM built-in 1 chip CPU (microcomputer) which carried out external [of the exterior ROM].
[0002]
[Description of the Prior Art] In recent years, in the computer system using a microcomputer (MPU or CPU), the so-called 1 chip CPU which contained various kinds of functions (LSI for a communication link, parallel I/OLSI, ROM, RAM, etc.) in the CPU body itself is used briskly. In case especially the ROM built-in 1 chip CPU constructs a small-scale system, it is used taking advantage of the merit that the miniaturization of a circuit can be measured. And what cannot rewrite the data which there are various kinds of things in ROM built in this 1 chip CPU, for example, were written in like a mask ROM at the time of manufacture, but is used for the general-purpose content of a program, the thing which can program only once by the user like the 1 time ROM, EPROM, E2 PROM, and the thing that can rewrite data freely like a flash memory are used according to each application. And these had the impossible protection function and it was useful that anything read the content of ROM through the external bus connected to CPU also in respect of security, such as confidentiality and safety. Therefore, although it was not impossible to have built the program which controls the whole system using such ROM built-in 1 chip CPU, either The possibility of nonconformity (existence of the bug which generates a program error) more nearly potential as the magnitude (shown by the number of steps) of a program becomes large as fate of a program also becomes high. And also on the occasion of partial modification which surely takes place when advancing employment of a program and going, the expensive ROM built-in 1 chip CPU itself had to be exchanged, and there was a problem also in cost. Generally from such a situation, it was used for it, having carried out external [of the rewritable exterior ROM] to the 1 chip CPU (one times ROM and EPROM, E2 PROM, flash memory, etc.). However, since there was no protection function like ROM with a built-in 1 chip CPU, from the data alteration from the outside etc., it was in the defenseless condition, and the problem on security called lowering of the secrecy nature of data and safety has arisen, and a certain solution was searched for.
[0003]
[Problem(s) to be Solved by the Invention] This invention is for solving the above troubles, and is offering the security system of the exterior ROM which secured the security of data by making the object in order to raise the security of the exterior ROM which carries out external to the ROM built-in 1 chip CPU, establishing a fixed-data field in Exterior ROM, and checking the data of said fixed-data field with the check means of ROM with a built-in 1 chip CPU.
[0004]
[Description of the Invention] The object of above-mentioned this invention is attained by the security system of the exterior ROM characterized by to form the check means (program) of the fixed-data field of said exterior ROM in said built-in ROM while it possesses the exterior ROM which has the fixed-data

field which was connected to the built-in ROM constituted so that it might be built in the 1 chip CPU and read-out might not be carried out from the outside, and said 1 chip CPU, and was set up beforehand.

[0005] Moreover, it is desirable to consider as the configuration which stored fixed data in the fixed address for performing the comparison with the data of the built-in ROM beforehand set as the fixed-data field of said exterior ROM. Moreover, it is desirable to consider as the configuration which stored in the fixed-data field of said exterior ROM the fixed data stored in the reserve field which the exterior ROM concerned has.

[0006] Moreover, it is desirable to consider as the configuration which stored in the fixed-data field of said exterior ROM the number-of-counts data of the byte count of the reserve field which the exterior ROM concerned has. Moreover, it is desirable to consider as the configuration which stored in the fixed-data field of said exterior ROM the error detection sign to all the fields that the exterior ROM concerned has.

[0007]

[Function] Namely, if it is in the security system of the exterior ROM made to constitute like the above The fixed data of the fixed-data field of the exterior ROM which the 1 chip CPU side recognizes with a check means whether they are the fixed data beforehand set up into program execution Check actuation, Namely, check actuation of the error detection sign to all the fields that the fixed data of the fixed address, the fixed data stored in a reserve field, the number-of-counts data of the byte count of a reserve field, and Exterior ROM have is performed. Among these, if at least one is inharmonious, the 1 chip CPU will be in a HOLD status, and actuation of the whole program will suspend it.

[0008] Thus, to the exterior ROM through which data may be rewritten, it may be altered, or the content may be looked into, even if you are among program execution, a check should always do with the check means by the side of the 1 chip CPU. (In case processing which specifically has a program by the side of Exterior ROM is performed, the 1 chip CPU side is surely accessed.) If coincidence of each fixed data is not checked, consequently it prevents from moving to activation, synthetic data and a synthetic system management -- secrecy-izing of restricted data and reservation of security can be attained -- can be performed.

[0009] That is, since the program itself stops if a check should be started (i.e., when there is possibility, such as alteration of the content), since it constituted so that check management of the content of data might be performed using the check means by the side of the 1 chip CPU also in the exterior ROM without a protection function, the safety of data is maintained.

[0010]

[Example] The explanatory view in which drawing 1 thru/or drawing 4 show one example of the security system of the exterior ROM concerning this invention, and drawing 1 explained the content stored in each field of the exterior ROM where the outline block diagram of this system and drawing 2 are used for the block diagram of a memory map, and drawing 3 is used for this system, and drawing 4 are flow drawings showing the flow of processing.

[0011] One is the 1 chip CPU among drawing 1 , and the built-in ROM 2 which has a protection function to data alteration is built in. And it has the check means (program) 3 so that it may mention later for this built-in ROM 2, and the fixed data stored in Exterior ROM are compared with the data in built-in ROM 2, and it is confirmed [coincidence and] whether it is inharmonious.

[0012] 4 is the exterior ROM accessed by this 1 chip CPU 1 by the external bus, and is constituted by program memory 5 and data memory 6. (In addition, some which are prepared in program memory 5 have this data memory 6.) And this program memory 5 and data memory 6 use the rewritable exterior ROM and ROM EPROM, for example, one times, E2 PROM, a flash memory, etc. if needed, respectively.

[0013] 7 is data memory constituted by the exterior RAM similarly connected to the 1 chip CPU 1 by the external bus, and is specifically constituted by S-RAM, D-RAM, false S-RAM, etc. The input section by which the equipment with which 8 is used for the communication link which a printer and 9 connect with a drop and 10 connects with the telephone line etc., and 11 are similarly constituted from a

calender / a clock function, and 12 is constituted from a ten key etc., and 13 are motor drives which the 1 chip CPU 1 drives directly.
[0014] In addition, the program of ROM built in the 1 chip CPU is written in as previous work business using a commercial ROM writer. At this event, reading of the content of the ROM and access to the content from the outside are possible. Moreover, it is confirmed using a verify function or a check function whether the content is written in correctly, and it makes the content of ROM after that the mode in which read-out is impossible by writing a specific command and data in the fixed address.
[0015] Hereafter, the memory map of drawing 2 is explained. Namely, as shown in drawing, built-in ROM 2 is constituted so that access of the content cannot be performed from an external bus after a program is written in by the ROM writer, as mentioned above. as the content -- initialization (concrete -- an I/O map --) of the 1 chip CPU 1 Data, such as counted value of the bit control approach of each port, and a timer, Fixed data, a check routine (comparing said fixed data by the side of Built-in ROM with the fixed data by the side of Exterior ROM and coincidence) It stores in the program for judging an inequality, a character font (font), and Exterior ROM, and routines, such as a translation table troubled if looked into by the third party, are stored.
[0016] Moreover, the value of the check digit (for example, CRC and a checksum) to the location and external ROM all field which store the value which counted the number of a main program, fixed data (what is compared with the fixed data by the side of said built-in ROM), a reserve field (for example, you may use in order to fill all as fixed data, such as FF, are also, and to make a judgment of coincidence and an inequality by the check routine by the side of Built-in ROM), and reserve fields etc. is stored in Exterior ROM.
[0017] Next, the content stored in each field of Exterior ROM using drawing 3 is explained. That is, the check routine by the side of Built-in ROM accesses the field of (1), (3), (5), (7), and (9), and the fixed data in comparison with the fixed data by the side of Built-in ROM (coincidence or inequality) are stored in it. A main program is stored in the field of (2), (4), (6), (8), and (10).
[0018] It is the reserve field where the main program remained in the field of (11), and is buried with patterns, such as FF decided beforehand. The byte count of the reserve field of (11) is stored in the field of (12). (For example, it will be set to C8H if it is 200 bytes) The CRC value which is a check digit to an external ROM all field is stored in the field of (13).
[0019] Hereafter, concrete processing of operation is explained using flow drawing of drawing 4 .
(1) after power-on and Exterior ROM -- 1 byte -- or read 2 bytes (step 1)
(2) Has initialization of the 1 chip CPU finished or not? (Step 2)
(3) the case where step 2 is NO -- an initialization parameter -- the exterior -- ROM .
[0020] (Step 3)
(4) When step 3 is NO, Built-in ROM is referred to, initialization of the 1 chip CPU is performed as it is also with the initialization parameter which Built-in ROM has, and subsequently (step 4) an initialization flag is set (step 5), and return to the initialization exit status of the 1 chip CPU.
(5) When step 3 is YES, Exterior ROM is referred to, a parameter is set and a number of parameters (step 6) counts. (Step 7)
In addition, the parameter of Exterior ROM shall be initialized, while it shall be enciphered and decoding at any time.
(6) the count of a number of parameters -- termination . (Step 8)
(7) When step 8 is NO, shift to step 10.
(8) When step 8 is YES, an initialization flag is set (step 9) and return to the initialization exit status of the 1 chip CPU.
(9) the case where step 2 is YES -- external ROM access -- termination .
[0021] (Step 10)
(10) When step 10 is NO, calculate a checksum and a CRC value. In addition, the approach using other error detecting codes may be used. (Step 11)
(11) Do check fixed data or not? (Step 12)
(12) When step 12 is NO, go into the preceding paragraph of step 15.

(13) Are data right or not when step 12 is YES?
[0022] (Step 13)
(14) When step 13 is NO, set the abnormalities NG 1= 1 in data, and go into the preceding paragraph of step 15. In addition, it is the result of the fixed data of the address of Exterior ROM which can be known beforehand confirming whether to be the right or not, and NG 1= 0 is normal and NG 1= 1 is abnormalities. (Step 14)
(15) When step 13 is YES, do carry out FF value check or not?
[0023] (Step 15)
(16) When step 15 is NO, go into the step 20 preceding paragraph.
(17) the case where step 15 is YES -- FF . (Step 16)
(18) When step 16 is NO, carry out 2= 1 set of NG by that which is except FF (abnormalities), and go into the step 20 preceding paragraph. In addition, it is the result of the fixed data of the reserve field (for example, FF is stored) of Exterior ROM confirming whether to be the right or not, and NG 2= 0 serves as normal, and NG 2= 1 serves as abnormalities.
[0024] (Step 17)
(19) the case where step 16 is YES -- the number of FFs (byte count) -- O.K. . (Step 18)
(20) When step 18 is NO, the number of FFs (byte count) is judged that a difference is unusual, carry out 3= 1 set of NG, and go into the step 20 preceding paragraph. In addition, it is the result of the fixed data of the reserve field (for example, the total (byte count) of FF value is stored) of Exterior ROM confirming whether to be the right or not, and NG 3= 0 shows normal and NG 3= 1 shows abnormalities. (Step 19)
(21) the case where step 18 is YES -- the address Of Exterior ROM -- +1 -- or take +two and return to the preceding paragraph of step 1 after that (step 20).
(22) When step 10 is YES, they are a checksum value or a CRC value (other error detecting codes may be used.). Do ** O.K. or not? (Step 21)
(23) When step 21 is NO, display an error situation.
[0025] (Step 22)
(24) When step 21 is YES, are they NG 1= 0 or no (is it O.K.?)? In addition, it is the result of the fixed data of the address of Exterior ROM which can be known beforehand confirming whether to be the right or not, and NG 1= 0 serves as normal, and NG 1= 1 serves as abnormalities. (Step 23)
(25) When step 23 is NO, display an error situation.
[0026] (Step 22)
(26) When step 23 is YES, are they NG 2= 0 or no (is it O.K.?)? In addition, it is the result of the fixed data of the reserve field (for example, FF is stored) of Exterior ROM confirming whether to be the right or not, and NG 2= 0 serves as normal, and NG 2= 1 serves as abnormalities. (Step 24)
(27) When step 24 is NO, display an error situation.
[0027] (Step 22)
(28) When step 24 is YES, are they NG 3= 0 or no (is it O.K.?)? In addition, it is the result of the fixed data of the reserve field (for example, the total (byte count) of FF value is stored) of Exterior ROM confirming whether to be the right or not, and NG 3= 0 shows normal and NG 3= 1 shows abnormalities. (Step 25)
(29) When step 25 is NO, display an error situation.
[0028] (Step 22)
in addition, reset of CPUI/O should make the same said (23) carried out, (25), and (27) after the display of an error situation (step 27) -- CPU will be in a HOLD status after that. (Step 28)
In addition, if the result of each check of steps 21, 23, 24, and 25 is NG (abnormalities), CPU will reset own I/O (each bit of for example, parallel I/O is initialized) of CPU, and will change it into the condition immediately after the power-on of CPU. For example, the safety of a circuit is maintained, as a motor drive circuit is reset and a motor will not be in the condition of those without time splendid. And CPU makes the CPU itself a HOLD status henceforth. This microcomputer system serves as a halt of operation after this.

(30) When step 25 is YES (i.e., when the result of all the checks of steps 21, 23, 24, and 25 is normal), jump to the main program of Exterior ROM. (Step 26)
In addition, even if abnormalities are in which step of said steps 12, 13, 15, 16, and 18 in the program execution of Built-in ROM, activation (loading) is continued to the last address of Exterior ROM. Because, it is unusual, and if access is stopped promptly, since it will be judged that the address is an object for a check, it constitutes so that it may be made to perform to the last address at step 10.
[0029] thus, the inside of the program execution of Built-in ROM -- all the checks of said steps 12, 13, 15, 16, and 18 -- that is The fixed data with which the fixed data of the fixed-data field of the exterior ROM which the 1 chip CPU side recognizes were set up beforehand (step 13), (Check actuation (step 11) of the error detection sign to all the fields that Exterior ROM has) The fixed data (step 13) of the fixed address, the fixed data of FF value stored in a reserve field (step 16), It confirms one by one whether be number-of-counts data (step 18) of the byte count of a reserve field. After reading all the fields of Exterior ROM, if at least one of the NG1, NG2, and NG3 which are as a result of step 14, step 17, and step 19 is inharmonious, the 1 chip CPU will be in a HOLD status, and actuation of the whole program will suspend it.
[0030] Although the flow of a rough program can be held also for a third party if Exterior ROM is disassembled since the program which inherits processing from ROM with a built-in 1 chip CPU succeedingly, and controls the whole system is written to Exterior ROM Even if this third party applied the patch to the program of Exterior ROM and added other additional programs, in order that the inequality of the fixed data of Built-in ROM and Exterior ROM which were set up beforehand may become clear, the 1 chip CPU serves as a halt of a HOLD status, i.e., program actuation.
[0031] Consequently, synthetic data and a synthetic system management -- secrecy-izing of restricted data and reservation of security can be attained -- can be performed. Moreover, a third party's analyzing Exterior ROM, and thinking, when the address (step 26) succeeded from the 1 chip CPU is found is removing the 1 chip CPU first and using the 1 chip CPU of ICE (incircuit emulator) or the same manufacturer in the ROM-less mode. In this case, even if it is, since the initialization approach (for example, step 3 --, such as counted value of an I/O map, the bit control approach of each port, and a timer) of the 1 chip CPU cannot be learned, actuation of a system becomes unfixed and it does not operate to normal.
[0032] Moreover, if it stores in Exterior ROM, it is looked into by the third party and it designs so that it may access into the 1 chip CPU when performing processing which has the program of Exterior ROM by designing so that important manipulation routines, such as data with inconvenience and a translation table, etc. may be stored in the 1 chip CPU, even if the content of a program of Exterior ROM will be looked into by the third party, trouble does not occur at all.
[0033] That is, since the program itself stops if a check should be started (i.e., when there is possibility, such as alteration of the content), since it constituted so that check management of the content of data might be performed using the check means by the side of the 1 chip CPU also in the exterior ROM without a protection function, the safety of data is maintained.
[0034]
[Effect] The security system of the exterior ROM concerning this invention Since it constitutes so that the fixed data stored in the fixed-data field of Exterior ROM by the check means formed in the built-in ROM of the 1 chip CPU may be checked The fixed data of the fixed-data field of the exterior ROM which the 1 chip CPU side recognizes with a check means whether they are the fixed data beforehand set up into program execution Check actuation, Namely, check actuation of the error detection sign to all the fields that the fixed data of the fixed address, the fixed data stored in a reserve field, the number-of-counts data of the byte count of a reserve field, and Exterior ROM have is performed. Among these, if at least one is inharmonious, the 1 chip CPU will be in a HOLD status, and actuation of the whole program will suspend it.
[0035] Thus, to the exterior ROM through which data may be rewritten, or it may be altered, or may look into the content, even if you are among program execution, a check should always do with the check means by the side of the 1 chip CPU. (In case processing which specifically has a program by the

side of Exterior ROM is performed, the 1 chip CPU side is surely accessed.) If coincidence of each fixed data is not checked, consequently it prevents from moving to activation, synthetic data and a synthetic system management -- secrecy-izing of restricted data and reservation of security can be attained -- can be performed.

[0036] that is , since the program itself stop if an inequality should become clear by comparison of fixed data , namely , when there be possibility , such as alteration of the content , since it constitute so that check management of the content of data may be perform using the check means by the side of the 1 chip CPU also in the exterior ROM without a protection function , the safety of data have the various features , such as be maintain .

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the outline block diagram of the security system of the exterior ROM concerning this invention.
[Drawing 2] It is the block diagram of the memory map of the security system of the exterior ROM concerning this invention.
[Drawing 3] It is an explanatory view explaining the content stored in each field of the exterior ROM used for the security system of the exterior ROM concerning this invention.
[Drawing 4] It is flow drawing showing the flow of the processing in the security system of the exterior ROM concerning this invention.
[Description of Notations]
1 1 Chip CPU
2 Built-in ROM
3 Check Means
4 Exterior ROM
5 Program Memory
6 Data Memory

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平5－265866

(43)公開日　平成５年(1993)10月15日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	12/14	３２０　Ａ	9293－5B		
	12/16	３３０　Ｃ	7629－5B		
	15/78	５１０　Ｚ	7530－5L		

審査請求　未請求　請求項の数５(全　９　頁)

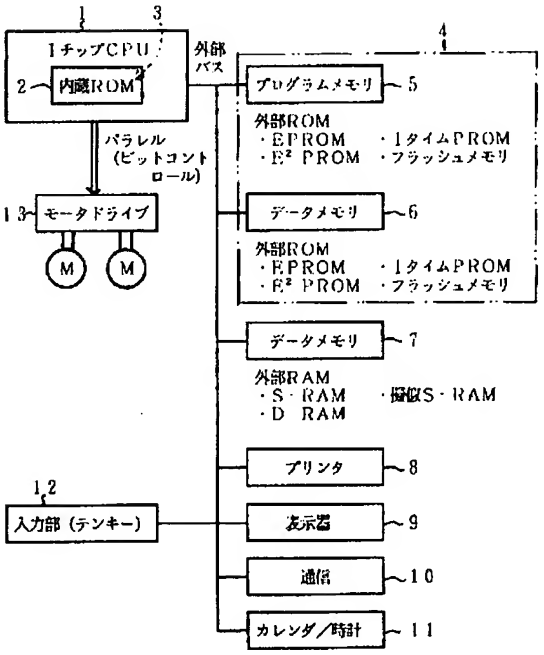
(21)出願番号　特願平4－63964

(22)出願日　平成４年(1992)３月19日

(71)出願人　000131201
株式会社シーエスケイ
東京都新宿区西新宿２丁目６番１号
(72)発明者　川村　孝之
東京都新宿区西新宿２－６－１　株式会社シーエスケイ内
(74)代理人　弁理士　宇高　克己

(54)【発明の名称】　外部ＲＯＭのセキュリティシステム

(57)【要約】
【目的】　ＲＯＭ内蔵型の１チップＣＰＵに外付けする外部ＲＯＭのセキュリティを高める為になされたものであり、外部ＲＯＭに固定データ領域を設け、１チップＣＰＵのＲＯＭのチェック手段で前記固定データ領域のデータをチェックすることによってデータのセキュリティを確保した外部ＲＯＭのセキュリティシステムを提供することである。
【構成】　１チップＣＰＵに内蔵され外部から読出し出来ないように構成した内蔵ＲＯＭと、前記１チップＣＰＵに接続され予め設定された固定データ領域を有する外部ＲＯＭとを具備すると共に前記内蔵ＲＯＭには前記外部ＲＯＭの固定データ領域のチェック手段を設けた外部ＲＯＭのセキュリティシステム。



1

【特許請求の範囲】
【請求項１】　１チップＣＰＵに内蔵され外部から読出し出来ないように構成した内蔵ＲＯＭと、前記１チップＣＰＵに接続され予め設定された固定データ領域を有する外部ＲＯＭとを具備すると共に前記内蔵ＲＯＭには前記外部ＲＯＭの固定データ領域のチェック手段を設けたことを特徴とする外部ＲＯＭのセキュリティシステム。
【請求項２】　前記外部ＲＯＭの固定データ領域に、予め設定された内蔵ＲＯＭのデータとの比較を行う為の固定アドレスの固定データを格納したことを特徴とする請求項１記載の外部ＲＯＭのセキュリティシステム。
【請求項３】　前記外部ＲＯＭの固定データ領域に、当該外部ＲＯＭが有する予備領域に格納する固定データを格納したことを特徴とする請求項１乃至２記載の外部ＲＯＭのセキュリティシステム。
【請求項４】　前記外部ＲＯＭの固定データ領域に、当該外部ＲＯＭが有する予備領域のバイト数のカウント数データを格納したことを特徴とする請求項１乃至３記載の外部ＲＯＭのセキュリティシステム。
【請求項５】　前記外部ＲＯＭの固定データ領域に、当該外部ＲＯＭが有する全ての領域に対するエラー検出符号を格納したことを特徴とする請求項１乃至４記載の外部ＲＯＭのセキュリティシステム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、外部ＲＯＭを外付けしたＲＯＭ内蔵型１チップＣＰＵ（マイクロコンピュータ）における、外部ＲＯＭの機密性、安全性を高めた外部ＲＯＭのセキュリティシステムに関するものである。
【０００２】
【従来の技術】近年、マイクロコンピュータ（ＭＰＵ又はＣＰＵ）を用いたコンピュータシステムにおいては、ＣＰＵ本体自身に各種の機能（通信用ＬＳＩ、パラレルＩ／ＯＬＳＩ、ＲＯＭ、ＲＡＭ等）を内蔵したいわゆる１チップＣＰＵが盛んに用いられている。特に、ＲＯＭ内蔵型の１チップＣＰＵは小規模のシステムを組む際に回路の小型化が計れるというメリットを活かして用いられている。そして、この１チップＣＰＵに内蔵されるＲＯＭには各種のものが有って、例えば、マスクＲＯＭのように製造時に書き込まれたデータを書き換えることはできず汎用的なプログラム内容に用いられるもの、１タイムＲＯＭのようにユーザにより１回だけプログラムが行なえるもの、ＥＰＲＯＭ、Ｅ² ＰＲＯＭ、フラッシュメモリ等のようにデータを自由に書き換えることができるものがそれぞれの用途に応じて使用されている。しかもこれらは何れのものもＣＰＵに接続される外部バスを経てＲＯＭ内容を読み出すことは不可能なプロテクト機能を有しており、機密性、安全性といったセキュリティの面でも有用であった。従って、このようなＲＯＭ内蔵型の１チップＣＰＵだけを用いてシステム全体を制御す

2

るプログラムを構築することも不可能ではなかったが、プログラムの宿命としてプログラムの規模（ステップ数で示される）が大きくなればなるほど潜在的な不具合（プログラムエラーを発生させるバグの存在）の可能性も高くなり、しかもプログラムの運用を進めて行く上で必ず起こる部分変更の際にも高価なＲＯＭ内蔵型の１チップＣＰＵ自体を交換しなければならずコスト的にも問題があった。このような事情から、一般的には書換が可能な外部ＲＯＭ（１タイムＲＯＭ、ＥＰＲＯＭ、Ｅ² ＰＲＯＭ、フラッシュメモリ等）を１チップＣＰＵに外付けして使用していた。しかしながら、１チップＣＰＵ内蔵のＲＯＭのようにプロテクト機能がないので、外部からのデータ変造等に対して無防備状態であり、データの秘匿性、安全性の低下といったセキュリティ上の問題が生じており何らかの解決策が求められていた。
【０００３】
【発明が解決しようとする課題】本発明は以上のような問題点を解決するためのものであり、その目的は、ＲＯＭ内蔵型の１チップＣＰＵに外付けする外部ＲＯＭのセキュリティを高める為になされたものであり、外部ＲＯＭに固定データ領域を設け、１チップＣＰＵ内蔵のＲＯＭのチェック手段で前記固定データ領域のデータをチェックすることによってデータのセキュリティを確保した外部ＲＯＭのセキュリティシステムを提供することである。
【０００４】
【発明の開示】上記本発明の目的は、１チップＣＰＵに内蔵され外部から読出し出来ないように構成した内蔵ＲＯＭと、前記１チップＣＰＵに接続され予め設定された固定データ領域を有する外部ＲＯＭとを具備すると共に前記内蔵ＲＯＭには前記外部ＲＯＭの固定データ領域のチェック手段（プログラム）を設けたことを特徴とする外部ＲＯＭのセキュリティシステムによって達成される。
【０００５】又、前記外部ＲＯＭの固定データ領域に、予め設定された内蔵ＲＯＭのデータとの比較を行う為の固定アドレスに固定データを格納した構成とすることが望ましい。又、前記外部ＲＯＭの固定データ領域に、当該外部ＲＯＭが有する予備領域に格納する固定データを格納した構成とすることが望ましい。
【０００６】又、前記外部ＲＯＭの固定データ領域に、当該外部ＲＯＭが有する予備領域のバイト数のカウント数データを格納した構成とすることが望ましい。又、前記外部ＲＯＭの固定データ領域に、当該外部ＲＯＭが有する全ての領域に対するエラー検出符号を格納した構成とすることが望ましい。
【０００７】
【作用】即ち、上記の如く構成させた外部ＲＯＭのセキュリティシステムにあっては、プログラムの実行中に、１チップＣＰＵ側が認識している外部ＲＯＭの固定デー

タ領域の固定データが予め設定された固定データであるか否かをチェック手段によってチェック操作、即ち固定アドレスの固定データ、予備領域に格納する固定データ、予備領域のバイト数のカウント数データ及び外部ＲＯＭが有する全ての領域に対するエラー検出符号のチェック操作を行い、この内１つでも不一致であるならば１チップＣＰＵはホールド状態となり、プログラム全体の動作が停止する。

【０００８】このようにデータを書換えたり、変造されたり或いは内容が覗かれる可能性のある外部ＲＯＭに対してはプログラムの実行中であっても常に１チップＣＰＵ側のチェック手段によってチェックがなされ、（具体的には外部ＲＯＭ側のプログラムがある処理を実行する際には必ず１チップＣＰＵ側にアクセスし、各固定データの一致が確認されなければ実行に移れないようにしておくものである）その結果、秘密データの秘匿化、セキュリティの確保が達成できる等総合的なデータやシステム管理が行なえる。

【０００９】即ち、プロテクト機能のない外部ＲＯＭにおいてもデータ内容のチェック管理を１チップＣＰＵ側のチェック手段を用いて行うように構成しているので、万一、チェックに掛かった場合即ち内容の変造等の可能性が有る場合にはプログラム自体がストップしてしまうのでデータの安全性は保たれるものである。

【００１０】

【実施例】図１乃至図４は、本発明に係る外部ＲＯＭのセキュリティシステムの一実施例を示すもので、図１は本システムの概略構成図、図２はメモリマップの構成図、図３は本システムに用いられる外部ＲＯＭの各領域に格納される内容を説明した説明図、図４は処理の流れを示すフロー図である。

【００１１】図１中、１は１チップＣＰＵであり、データ変造に対するプロテクト機能を有する内蔵ＲＯＭ２が内蔵されるものである。そしてこの内蔵ＲＯＭ２には後述する如くチェック手段（プログラム）３を有し、外部ＲＯＭ内に格納される固定データと内蔵ＲＯＭ２内のデータとを比較し一致、不一致であるかをチェックするものである。

【００１２】４は、この１チップＣＰＵ１に外部バスによってアクセスされる外部ＲＯＭであり、プログラムメモリ５とデータメモリ６により構成されている。（尚、このデータメモリ６がプログラムメモリ５内に設けられているものもある。）そして、このプログラムメモリ５及びデータメモリ６はそれぞれ必要に応じて書換が可能な外部ＲＯＭ例えば、１タイムＲＯＭ、ＥＰＲＯＭ、E^2ＰＲＯＭ、フラッシュメモリ等を使用するものである。

【００１３】７は同様に１チップＣＰＵ１に外部バスによって接続される外部ＲＡＭによって構成されるデータメモリであり、具体的には例えばＳ－ＲＡＭ、Ｄ－ＲＡＭ、擬似Ｓ－ＲＡＭ等によって構成されるものである。８は同様にプリンタ、９は表示器、１０は電話回線等と接続する通信に用いられる装置、１１はカレンダ／時計機能、１２はテンキー等で構成される入力部、１３は１チップＣＰＵ１が直接的に駆動するモータードライブである。

【００１４】尚、前作業として、１チップＣＰＵに内蔵されるＲＯＭのプログラムは市販のＲＯＭライタを用いて書き込まれるものである。この時点ではＲＯＭの内容の読込、外部からの内容へのアクセスは可能である。又、内容が正しく書き込まれているか否かがベリファイ機能又は、チェック機能を用いてチェックされ、その後、特定のコマンド、データを固定アドレスに書き込むことによってＲＯＭ内容を読出し不可能なモードにしておくものである。

【００１５】以下、図２のメモリマップについて説明する。即ち、図に示すように内蔵ＲＯＭ２は前述した如くＲＯＭライタによってプログラムが書き込まれた後に外部バスから内容のアクセスができないように構成されており、その内容としては１チップＣＰＵ１の初期化（具体的にはＩ／Ｏマップ、各ポートのビットコントロール方法、タイマーのカウント値等のデータ）、固定データ、チェックルーチン（内蔵ＲＯＭ側の前記固定データと外部ＲＯＭ側の固定データとを比較し一致、不一致の判断を行う為のプログラム）、文字フォント（字体）、外部ＲＯＭ内に格納しておき第三者に覗かれては困る例えば変換テーブル等のルーチンが格納されている。

【００１６】又、外部ＲＯＭにはメインプログラム、固定データ（前記内蔵ＲＯＭ側の固定データと比較されるもの）、予備領域（例えば全てＦＦ等の固定データでもって埋め尽くしておいて内蔵ＲＯＭ側のチェックルーチンで一致、不一致の判断を行う為に用いても良い）、予備領域の数をカウントした値を格納する場所、外部ＲＯＭ全領域に対するチェックデジット（例えばＣＲＣやチェックサム）の値等が格納されている。

【００１７】次に図３を用いて外部ＲＯＭの各領域に格納される内容を説明する。即ち、（１）、（３）、（５）、（７）、（９）の領域には内蔵ＲＯＭ側のチェックルーチンがアクセスして内蔵ＲＯＭ側の固定データと比較（一致又は不一致）する固定データが格納される。（２）、（４）、（６）、（８）、（１０）の領域にはメインプログラムが格納される。

【００１８】（１１）の領域にはメインプログラムの余った予備領域であって、予め決められたＦＦ等のパターンによって埋められる。（１２）の領域には（１１）の予備領域のバイト数を格納する。（例えば２００バイトとするとＣ８Ｈとなる）（１３）の領域には外部ＲＯＭ全領域に対するチェックデジットであるＣＲＣ値が格納される。

【００１９】以下、図４のフロー図を用いて具体的な動

作処理の説明をする。
（1）パワーオンの後、外部ROMを1バイト又は2バイト読み込む（ステップ1）
（2）1チップCPUの初期化が終わっているか否か。
（ステップ2）
（3）ステップ2がNOの場合、初期化パラメータは外部ROMか否か。
【0020】（ステップ3）
（4）ステップ3がNOの場合、内蔵ROMが参照され、内蔵ROMが持っている初期化パラメータでもって1チップCPUの初期化が実行され、（ステップ4）次いで初期化フラグがセットされて（ステップ5）、1チップCPUの初期化終了状態に戻る。
（5）ステップ3がYESの場合、外部ROMが参照され、パラメータがセットされ、（ステップ6）パラメータ数がカウントされる。（ステップ7）
尚、外部ROMのパラメータは暗号化されているものとし随時解読しながら初期化するものとする。
（6）パラメータ数のカウント終了か否か。
（ステップ8）
（7）ステップ8がNOの場合、ステップ10に移行する。
（8）ステップ8がYESの場合、初期化フラグがセットされて（ステップ9）、1チップCPUの初期化終了状態に戻る。
（9）ステップ2がYESの場合、外部ROMアクセス終了か否か。
【0021】（ステップ10）
（10）ステップ10がNOの場合、チェックサム、CRC値を計算する。尚、他の誤り検出符号を用いた方法を用いても良い。（ステップ11）
（11）固定データをチェックするか否か。
（ステップ12）
（12）ステップ12がNOの場合、ステップ15の前段へ入る。
（13）ステップ12がYESの場合、データが正しいか否か。
【0022】（ステップ13）
（14）ステップ13がNOの場合、データ異常NG1＝1をセットしステップ15の前段へ入る。尚、外部ROMの予め知り得るアドレスの固定データが正しいか否かをチェックした結果であり、NG1＝0が正常、NG1＝1が異常。（ステップ14）
（15）ステップ13がYESの場合、FF値チェックするか否か。
【0023】（ステップ15）
（16）ステップ15がNOの場合、ステップ20前段へ入る。
（17）ステップ15がYESの場合、FFか否か。
（ステップ16）
（18）ステップ16がNOの場合、FF以外である（異常）のでNG2＝1セットし、ステップ20前段へ入る。尚、外部ROMの予備領域（例えばFFが格納されている）の固定データが正しいか否かチェックした結果であり、NG2＝0が正常、NG2＝1が異常となる。
【0024】（ステップ17）
（19）ステップ16がYESの場合、FFの数（バイト数）OKか否か。（ステップ18）
（20）ステップ18がNOの場合、FFの数（バイト数）が異なり異常と判断され、NG3＝1セットし、ステップ20前段へ入る。尚、外部ROMの予備領域（例えばFF値の総数（バイト数）が格納されている）の固定データが正しいか否かチェックした結果であり、NG3＝0が正常、NG3＝1が異常を示す。
（ステップ19）
（21）ステップ18がYESの場合、外部ROMのアドレスを＋1、又は＋2して、（ステップ20）その後ステップ1の前段に戻る。
（22）ステップ10がYESの場合、チェックサム値又はCRC値（他の誤り検出符号を用いても良い。はOKか否か。（ステップ21）
（23）ステップ21がNOの場合、エラー状態の表示を行う。
【0025】（ステップ22）
（24）ステップ21がYESの場合、NG1＝0か（OKか）否か。尚、外部ROMの予め知り得るアドレスの固定データが正しいか否かをチェックした結果であり、NG1＝0が正常、NG1＝1が異常となる。（ステップ23）
（25）ステップ23がNOの場合、エラー状態の表示を行う。
【0026】（ステップ22）
（26）ステップ23がYESの場合、NG2＝0か（OKか）否か。尚、外部ROMの予備領域（例えばFFが格納されている）の固定データが正しいか否かチェックした結果であり、NG2＝0が正常、NG2＝1が異常となる。（ステップ24）
（27）ステップ24がNOの場合、エラー状態の表示を行う。
【0027】（ステップ22）
（28）ステップ24がYESの場合、NG3＝0か（OKか）否か。尚、外部ROMの予備領域（例えばFF値の総数（バイト数）が格納されている）の固定データが正しいか否かチェックした結果であり、NG3＝0が正常、NG3＝1が異常を示す。（ステップ25）

（２９）ステップ２５がＮＯの場合、エラー状態の表示を行う。

【００２８】（ステップ２２）

尚、前記した（２３）、（２５）、（２７）も同様にエラー状態の表示の後ＣＰＵＩ／Ｏのリセットがなされ（ステップ２７）、その後ＣＰＵはホールド状態となる。（ステップ２８）

尚、ステップ２１、２３、２４、２５の各々のチェックの結果がＮＧ（異常）であるなら、ＣＰＵはＣＰＵ自身のＩ／Ｏ（例えば、パラレルＩ／Ｏの各ビットを初期化）をリセットし、ＣＰＵのパワーオン直後の状態にする。例えばモータードライブ回路をリセットし、モータが回りっぱなしの状態にならないようにして回路の安全性を保つ。そして、以後ＣＰＵはＣＰＵ自身をホールド状態にする。これ以後このマイクロコンピュータシステムは動作停止となる。

（３０）ステップ２５がＹＥＳの場合、即ち、ステップ２１、２３、２４、２５の全てのチェックの結果が正常である場合には、外部ＲＯＭのメインプログラムへジャンプする。（ステップ２６）

尚、内蔵ＲＯＭのプログラムの実行中に前記ステップ１２、１３、１５、１６、１８の何れかのステップに異常があっても外部ＲＯＭの最終アドレスまで実行（ロード）は続けられる。なぜならば、異常で直ちにアクセスを停止させてしまうとそのアドレスがチェック対象であると判断されてしまう為ステップ１０で最後のアドレスまで実行させるように構成するものである。

【００２９】このように、内蔵ＲＯＭのプログラムの実行中に前記ステップ１２、１３、１５、１６、１８の全てのチェック即ち、１チップＣＰＵ側が認識している外部ＲＯＭの固定データ領域の固定データが予め設定された固定データ（ステップ１３）、（外部ＲＯＭが有する全ての領域に対するエラー検出符号のチェック操作（ステップ１１）、固定アドレスの固定データ（ステップ１３）、予備領域に格納するＦＦ値の固定データ（ステップ１６）、予備領域のバイト数のカウント数データ（ステップ１８））であるか否かのチェックを順次行い、外部ＲＯＭの全領域を読んだ後、ステップ１４、ステップ１７、ステップ１９での結果であるＮＧ１、ＮＧ２、ＮＧ３の１つでも不一致であるならば１チップＣＰＵはホールド状態となり、プログラム全体の動作が停止する。

【００３０】外部ＲＯＭには、１チップＣＰＵ内蔵のＲＯＭから引続いて処理を受け継いで、システム全体を制御するプログラムが書かれているので、外部ＲＯＭを逆アセンブルすれば大まかなプログラムの流れを第三者にも掴めるが、この第三者が外部ＲＯＭのプログラムにパッチを当てて、他の追加プログラムを書き加えたとしても予め設定した内蔵ＲＯＭと外部ＲＯＭとの固定データの不一致が判明する為に１チップＣＰＵはホールド状態即ちプログラム動作の停止となる。

【００３１】その結果、秘密データの秘匿化、セキュリティの確保が達成できる等総合的なデータやシステム管理が行なえる。又、第三者が外部ＲＯＭを解析して、１チップＣＰＵから引き継ぐアドレス（ステップ２６）を見つけた場合、考えられることは、先ず１チップＣＰＵを外し、ＩＣＥ（インサーキットエミュレータ）や同一メーカーの１チップＣＰＵをＲＯＭ無しモードで用いることである。この場合にあっても、１チップＣＰＵの初期化方法（例えば、Ｉ／Ｏマップ、各ポートのビットコントロール方法、タイマーのカウント値等ステップ３…）を知ることができない為にシステムの動作が不定となり正常に作動することはない。

【００３２】又、外部ＲＯＭに格納し、第三者に覗かれては不都合があるデータや変換テーブル等の重要な処理ルーチン等は１チップＣＰＵ内に格納するように設計することによって、外部ＲＯＭのプログラムがある処理を実行するとき必ず１チップＣＰＵ内にアクセスしなければならないように設計しておけば外部ＲＯＭのプログラム内容が第三者によって覗かれても何ら支障は起きない。

【００３３】即ち、プロテクト機能のない外部ＲＯＭにおいてもデータ内容のチェック管理を１チップＣＰＵ側のチェック手段を用いて行うように構成しているので、万一、チェックに掛かった場合即ち内容の変造等の可能性が有る場合にはプログラム自体がストップしてしまうのでデータの安全性は保たれるものである。

【００３４】

【効果】本発明に係る外部ＲＯＭのセキュリティシステムは、１チップＣＰＵの内蔵ＲＯＭに設けられたチェック手段によって外部ＲＯＭの固定データ領域に格納される固定データをチェックするように構成しているので、プログラムの実行中に、１チップＣＰＵ側が認識している外部ＲＯＭの固定データ領域の固定データが予め設定された固定データであるか否かをチェック手段によってチェック操作、即ち固定アドレスの固定データ、予備領域に格納する固定データ、予備領域のバイト数のカウント数データ及び外部ＲＯＭが有する全ての領域に対するエラー検出符号のチェック操作を行い、この内１つでも不一致であるならば１チップＣＰＵはホールド状態となり、プログラム全体の動作が停止する。

【００３５】このようにデータを書換えたり、変造されたり或いは内容を覗こうとする可能性のある外部ＲＯＭに対してはプログラムの実行中であっても常に１チップＣＰＵ側のチェック手段によってチェックがなされ、（具体的には外部ＲＯＭ側のプログラムがある処理を実行する際には必ず１チップＣＰＵ側にアクセスし、各固定データの一致が確認されなければ実行に移れないようにしておくものである）その結果、秘密データの秘匿化、セキュリティの確保が達成できる等総合的なデータやシステム管理が行なえる。

9　　10

【００３６】即ち、プロテクト機能のない外部ＲＯＭにおいてもデータ内容のチェック管理を１チップＣＰＵ側のチェック手段を用いて行うように構成しているので、万一、固定データの比較によって不一致が判明した場合、即ち内容の変造等の可能性が有る場合にはプログラム自体がストップしてしまうのでデータの安全性は保たれる等種々の特長を有する。

【図面の簡単な説明】

【図１】本発明に係る外部ＲＯＭのセキュリティシステムの概略構成図である。

【図２】本発明に係る外部ＲＯＭのセキュリティシステムのメモリマップの構成図である。

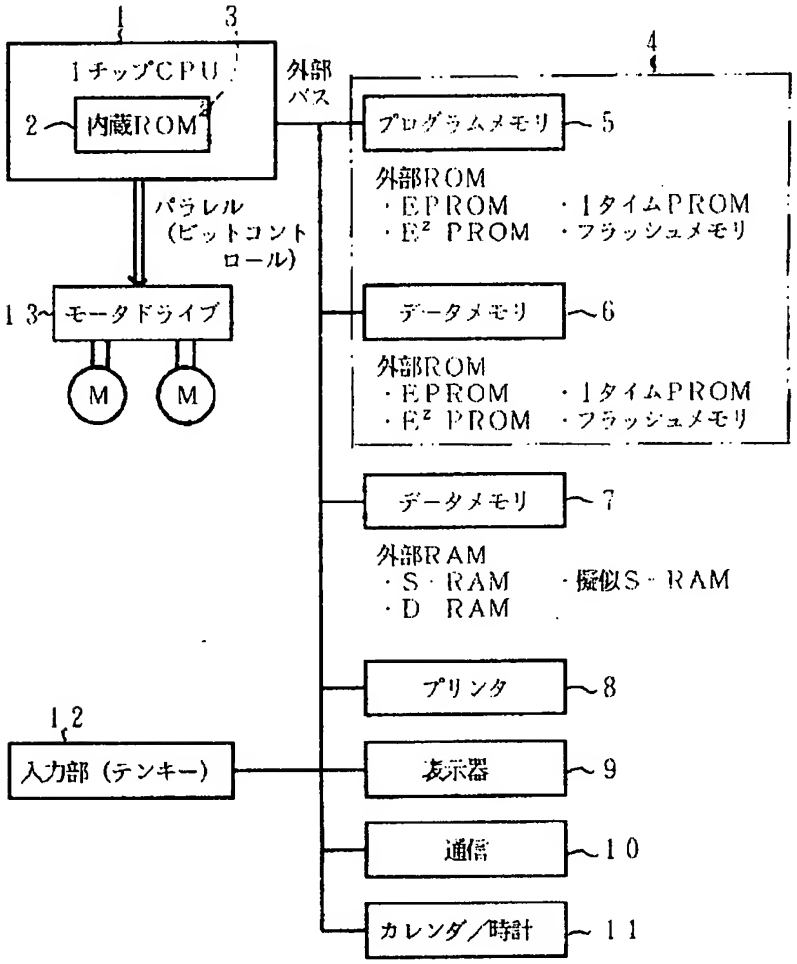
【図３】本発明に係る外部ＲＯＭのセキュリティシステムに用いられる外部ＲＯＭの各領域に格納される内容を説明した説明図である。

【図４】本発明に係る外部ＲＯＭのセキュリティシステムにおける処理の流れを示すフロー図である。

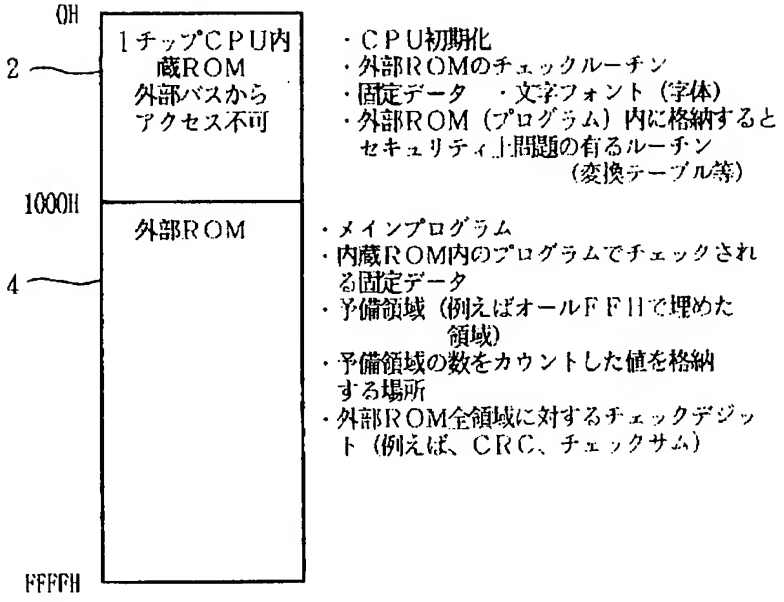
【符号の説明】

1	１チップＣＰＵ
2	内蔵ＲＯＭ
3	チェック手段
4	外部ＲＯＭ
5	プログラムメモリ
6	データメモリ

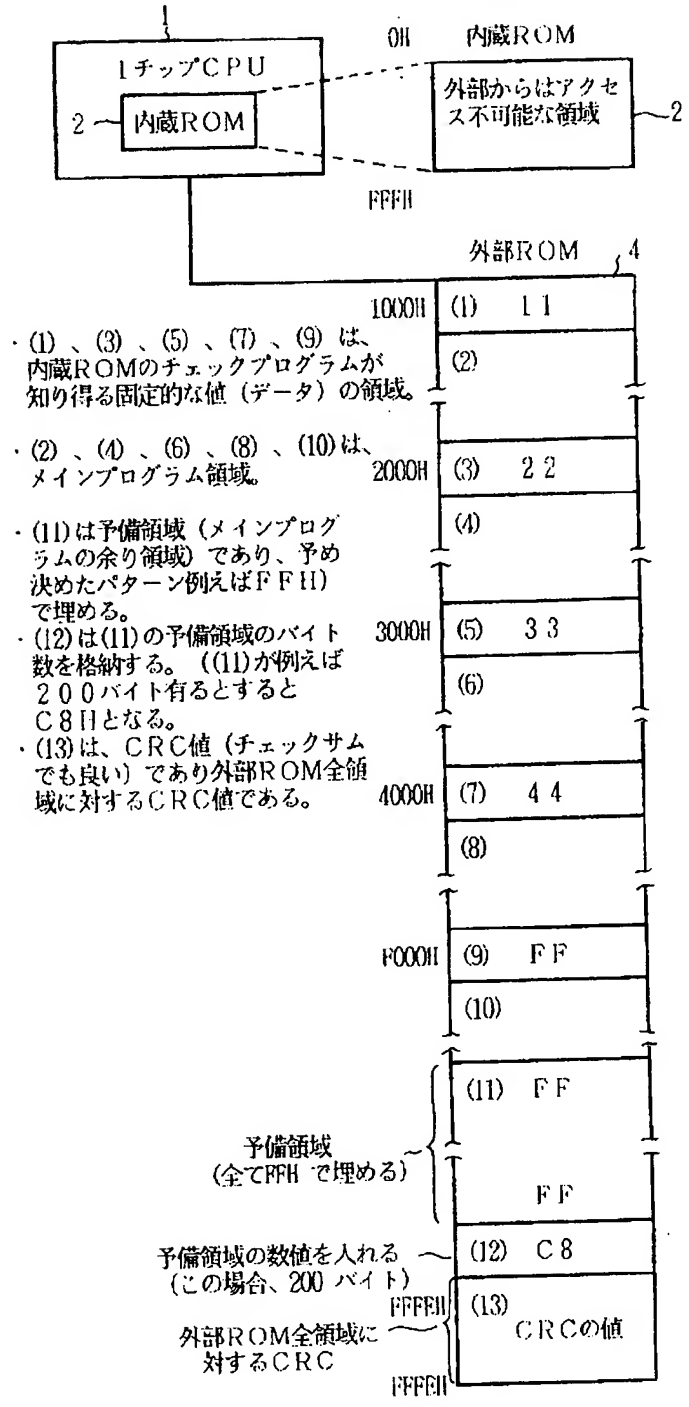
【図１】



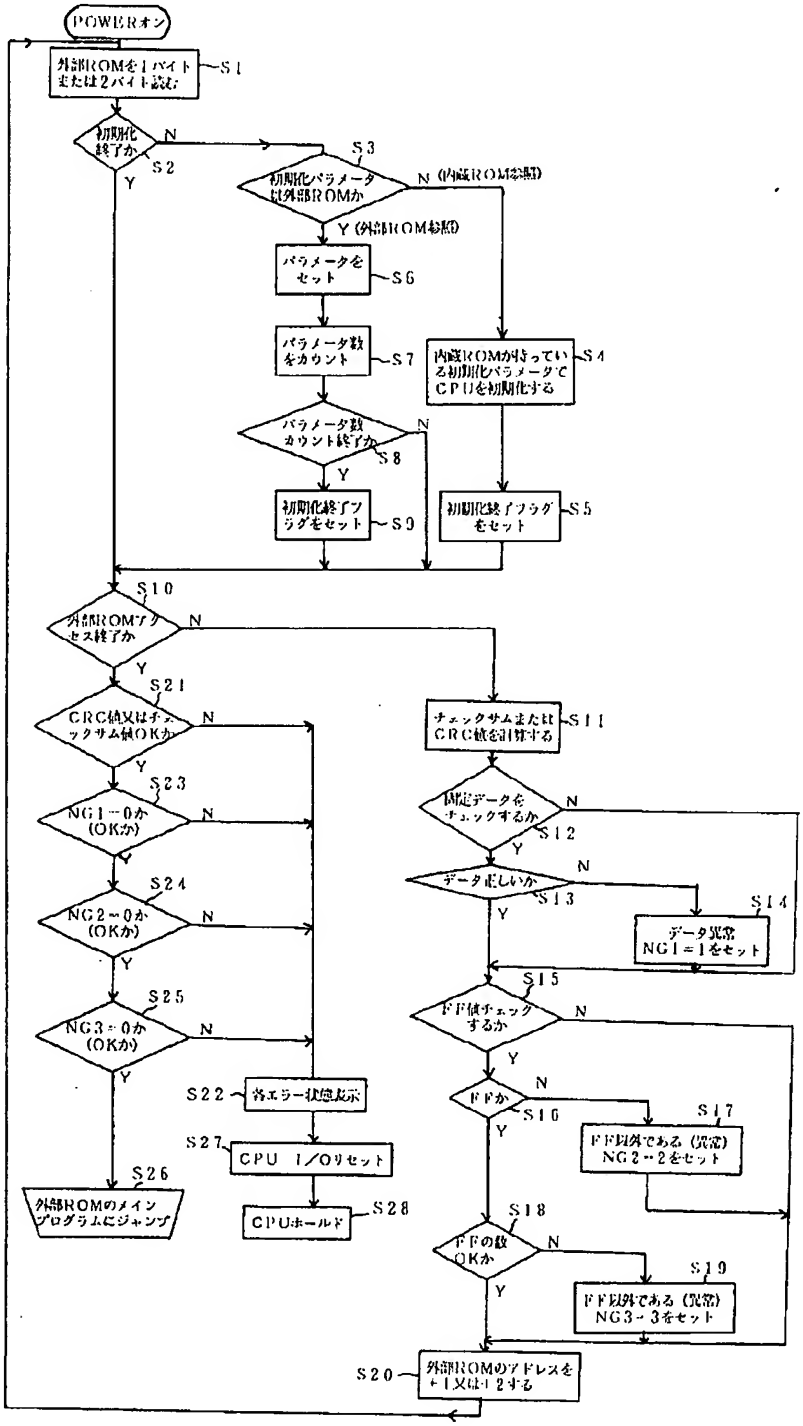
【図2】


0H
1チップCPU内蔵ROM
外部バスからアクセス不可
2
1000H
外部ROM
4
FFFFH
・CPU初期化
・外部ROMのチェックルーチン
・固定データ　・文字フォント（字体）
・外部ROM（プログラム）内に格納するとセキュリティ上問題の有るルーチン（変換テーブル等）
・メインプログラム
・内蔵ROM内のプログラムでチェックされる固定データ
・予備領域（例えばオールFFHで埋めた領域）
・予備領域の数をカウントした値を格納する場所
・外部ROM全領域に対するチェックデジット（例えば、CRC、チェックサム）

【図3】


1
1チップCPU
2
内蔵ROM
0H
内蔵ROM
外部からはアクセス不可能な領域
2
FFFH
外部ROM
4
1000H
(1) 11
(2)
2000H
(3) 22
(4)
3000H
(5) 33
(6)
4000H
(7) 44
(8)
F000H
(9) FF
(10)
(11) FF
FF
予備領域
(全てFFH で埋める)
予備領域の数値を入れる
(この場合、200 バイト)
(12) C8
FFFEH
(13)
CRCの値
外部ROM全領域に対するCRC
FFFFH
・(1)、(3)、(5)、(7)、(9)は、内蔵ROMのチェックプログラムが知り得る固定的な値（データ）の領域。
・(2)、(4)、(6)、(8)、(10)は、メインプログラム領域。
・(11)は予備領域（メインプログラムの余り領域）であり、予め決めたパターン例えばFFH）で埋める。
・(12)は(11)の予備領域のバイト数を格納する。（(11)が例えば200バイト有るとするとC8Hとなる。
・(13)は、CRC値（チェックサムでも良い）であり外部ROM全領域に対するCRC値である。

【図4】


POWERオン
外部ROMを1バイトまたは2バイト読む
S1
初期化終了か
N
Y
S2
S3
初期化パラメータは外部ROMか
N (内蔵ROM参照)
Y (外部ROM参照)
パラメータをセット
S6
パラメータ数をカウント
S7
内蔵ROMが持っている初期化パラメータでCPUを初期化する
S4
パラメータ数カウント終了か
S8
初期化終了フラグをセット
S9
初期化終了フラグをセット
S5
S10
外部ROMアクセス終了か
S21
CRC値又はチェックサム値OKか
S23
NG1＝0か(OKか)
S24
NG2＝0か(OKか)
S25
NG3＝0か(OKか)
S22
各エラー状態表示
S27
CPU I/Oリセット
CPUホールド
S28
S26
外部ROMのメインプログラムにジャンプ
チェックサムまたはCRC値を計算する
S11
固定データをチェックするか
S12
データ正しいか
S13
S14
データ異常NG1＝1をセット
S15
FF値チェックするか
FFか
S16
S17
FF以外である（異常）NG2＝2をセット
FFの数OKか
S18
S19
FF以外である（異常）NG3＝3をセット
S20
外部ROMのアドレスを+1又は+2する